



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/915,511	07/26/2001	Michael Wayne Brown	AUS920010528US1	6703

43307 7590 07/25/2005

IBM CORP (AP)
C/O AMY PATTILLO
P. O. BOX 161327
AUSTIN, TX 78716

EXAMINER

WILLIAMS, JEFFERY L

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 07/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/915,511

Applicant(s)

BROWN ET AL:

Examiner

Jeffery Williams

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 April 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-38 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-38 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 28 September 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2/07/05.
- ☒ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 4/25/2005.

All rejections not set forth below have been withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1 – 5, 7 – 9, 11 – 13, 15 – 17, 19 – 21, 23 – 25, and 27 - 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeSimone et al., US Patent: 6,212,548 B1 in view of Smithies et al., US Patent: 6,091,835.

Regarding claim 1, DeSimone et al. discloses a method for enabling a messaging session comprising a plurality of users participating in the session. The participating users are able to view the history of the messaging session in the form of a 'conversation', a string of recorded messages (Col. 2, lines 48-56; Col. 3, lines 43-53). DeSimone et al. does not disclose that the messaging session is verifiable by attaching digital signatures of the participants to the recording of the session. DeSimone et al.,

1 however, does teach the understanding that certain messaging sessions between users
2 may need measures of security provided (Col. 14, lines 50-54).

3 Smithies et al. discloses a method for recording a verifiable transcript of
4 statements, transactions, or events between parties by attaching digital signatures of
5 the participants to the transcript (Col. 3, lines 40-61; Col. 41, lines 21-36).

6 To combine the method for enabling a messaging session and a history of the
7 session between participants with a method for recoding digital signatures of
8 participants along with the transcript would provide a needed measure of security.

9 Therefore, it would have been obvious to one ordinarily skilled in the art to combine the
10 method of DeSimone et al. with the method of Smithies et al., because it is obvious that
11 certain messaging sessions between users will require the level of verifiability and
12 accountability that a digitally signed transcript would provide.

13
14 Regarding claim 2, the combination of DeSimone et al. and Smithies et al.
15 discloses the recording of the selection of message entries and attaching the plurality of
16 digital signatures at a messaging server system connected via a network to a plurality of
17 client systems accessible to the plurality of users (Smithies et al., Fig. 2, Col. 3, lines
18 40-61; Col. 9, lines 56-63; Col. 41, lines 21-36). As shown by Smithies et al., the
19 transcript generator module may reside on a system other than a client system that has
20 access to it. In this case, digital signatures from a plurality of interacting client systems
21 will be attached at the messaging server system.

22

1 Regarding claim 3, the combination of DeSimone et al. and Smithies et al.
2 discloses the recording of the selection of message entries and attaching the plurality of
3 digital signatures at a client system connected via a network to a plurality of client
4 systems accessible to the plurality of users (Smithies et al., Fig. 1, Col. 3, lines 40-61;
5 Col. 8, lines 15-40; Col. 41, lines 21-36). As shown by Smithies et al., when the client
6 application and the transcript generator module both reside on the client system, then
7 the digital signatures will be attached at the client system.

8
9 Regarding claim 4, the combination of DeSimone et al. and Smithies et al.
10 discloses a method for verifying a messaging session, wherein verifying includes at
11 least one of verifying at least one of a plurality of digital signatures and verifying an
12 integrity of the messaging session (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col.
13 11, lines 44-67). As disclosed by Smithies et al., the transcript generator module will
14 perform session verification functions upon the transcript, such as verification of
15 signatures and verification of the transcript checksum.

16
17 Regarding claim 5, the combination of DeSimone et al. and Smithies et al.
18 discloses a method for transmitting a request to a plurality of users to each attach a
19 digital signature to a recording of a selection of message entries from a messaging
20 session. (Smithies et al., Col. 41, lines 21-36, Col. 44, lines 46-56). As disclosed by
21 Smithies et al., multiple parties, or users, can engage in the generation of a transcript.

1 The transcript generator module will request participants to the session to provide their
2 digital signatures to the transcript.

3
4 Regarding claim 7, the combination of DeSimone et al. and Smithies et al.
5 discloses a method for calculating a checksum for the recording of the selection of
6 message entries from the messaging session; and encrypting the checksum utilizing a
7 private key for a particular digital signature from among the plurality of digital signatures,
8 wherein a particular public key is enabled to decrypt the encrypted checksum (Smithies
9 et al., Col. 8, lines 24-43; Col. 14, lines 26-39).

10
11 Regarding claim 8, the combination of DeSimone et al. and Smithies et al.
12 discloses a method for verifying an integrity of a selection of message entries by
13 calculating a current checksum for the selection of the plurality of message entries;
14 decrypting said encrypted checksum with a particular public key; and comparing the
15 current checksum with the decrypted checksum, wherein the integrity is verified if the
16 decrypted checksum matches the current checksum (Smithies et al., Col. 14, lines 26-
17 39).

18
19 Regarding claim 9, the combination of DeSimone et al. and Smithies et al.
20 discloses a method for verifying a particular digital signature from among a plurality of
21 digital signatures in order to verify a particular user from among a plurality of users

1 associated with the particular digital signature (Smithies et al., Col. 41, lines 7-13, 21-
2 36).

3
4 Regarding claim 11, DeSimone et al. discloses a system for recording a
5 message session comprising a server system communicatively connected to a network
6 (Col. 3, line 43 – Col. 4, line 18). DeSimone et al. does not disclose the server system
7 comprising means to record the selection of message entries and means for attaching
8 the digital signatures of the session participants to the recording of the selection of
9 message entries.

10 Smithies et al. discloses means to record a transcript (the selection of message
11 entries from the plurality of users) as well as a means for attaching the digital signatures
12 of the session participants to the recording of the selection of message entries (Col. 7,
13 lines 41-50; Col. 24, lines 48-55; Col. 41, lines 24-35; Col. 41, line 64 - Col. 42, line 37).
14 As disclosed by Smithies et al., communicating parties can digitally sign a transcript,
15 generated by a transcript generator module that is residing on a server.

16 The combination of the methods of DeSimone et al. and Smithies et al., as
17 explained regarding claim 1, would obviously be utilized in a system. Thus, it would
18 have been obvious to one ordinarily skilled in the art to combine the system of
19 DeSimone et al. with the system of Smithies et al., because it is obvious that certain
20 systems that record messaging sessions between users will require the level of
21 verifiability and accountability that a system utilizing a digitally signed transcript would
22 provide.

1
2 Regarding claim 12, the combination of DeSimone et al. and Smithies et al.
3 discloses a logging controller for verifying a messaging session, wherein the verifying
4 includes at least one of verifying at least one of a plurality of digital signatures and
5 verifying an integrity of the messaging session (Smithies et al., Col. 9, line 64 – Col. 10,
6 line 9; Col. 11, lines 44-67). As disclosed by Smithies et al., the transcript generator
7 module will perform session verification functions upon the transcript, such as
8 verification of signatures and verification of the transcript checksum.

9
10 Regarding claim 13, the combination of DeSimone et al. and Smithies et al.
11 discloses a system means for transmitting a request to a plurality of users to each
12 attach a digital signature to a recording of a selection of message entries from a
13 messaging session. (Smithies et al., Col. 41, lines 21-36, Col. 44, lines 46-56). In the
14 system, as disclosed by Smithies, multiple parties, or users, can engage in the
15 generation of a transcript. The transcript generator module will request participants to
16 the session to provide their digital signatures to the transcript.

17
18 Regarding claim 15, the combination of DeSimone et al. and Smithies et al.
19 discloses a system means for calculating a checksum for the recording of a selection of
20 message entries from a messaging session; and means for encrypting a checksum
21 utilizing a private key for a particular digital signature from among a plurality of digital

1 signatures, wherein a particular public key is enabled to decrypt the encrypted
2 checksum (Smithies et al., Col. 8, lines 24-43; Col. 14, lines 26-39).

3
4 Regarding claim 16, the combination of DeSimone et al. and Smithies et al.
5 discloses a system means for verifying an integrity of a selection of a plurality of
6 message entries by calculating a current checksum for the selection of the plurality of
7 message entries; decrypting said encrypted checksum with a particular public key; and
8 comparing the current checksum with the decrypted checksum, wherein the integrity is
9 verified if the decrypted checksum matches the current checksum (Smithies et al., Col.
10 14, lines 26-39).

11
12 Regarding claim 17, the combination of DeSimone et al. and Smithies et al.
13 discloses a system means for verifying a particular digital signature from among a
14 plurality of digital signatures in order to verify a particular user from among a plurality of
15 users associated with the particular digital signature (Smithies et al., Col. 41, lines 7-13,
16 21-36).

17
18 Regarding claim 19, DeSimone et al. discloses both a method and system
19 implementing the method for recording a message session, as explained in claims 1
20 and 11. DeSimone et al. does not directly disclose the system utilizing a method that
21 has been implemented in a program residing on a computer readable medium.

1 Smithies et al. discloses a program means for enabling a recording of a transcript
2 (the selection of message entries from the plurality of users) as well as a program
3 means for attaching the digital signatures of the session participants to the recording of
4 the selection of message entries (Col. 7, lines 41-50; Col. 24, lines 48-55; Col. 41, lines
5 24-35; Col. 41, line 64 - Col. 42, line 37). As disclosed by Smithies et al.,
6 communicating parties can digitally sign a transcript by running browser software
7 enhanced by Java code downloaded from a server.

8 The combination of the methods/systems of DeSimone et al. and Smithies et al.,
9 as explained regarding claims 1 and 11, would obviously incorporate a program means
10 and a computer readable medium embodied by the program means. Thus, it would
11 have been obvious to one ordinarily skilled in the art to combine the system/method
12 means of DeSimone et al. with the system/method/program means of Smithies et al.,
13 because it is obvious that systems utilizing methods for recording messaging sessions
14 between users will require program means for practical implementation.

15
16 Regarding claim 20, the combination of DeSimone et al. and Smithies et al.
17 discloses program means for enabling verification of a messaging session, wherein
18 verifying includes at least one of verifying at least one of a plurality of digital signatures
19 and verifying an integrity of the messaging session. (Smithies et al., Col. 9, line 64 –
20 Col. 10, line 9; Col. 11, lines 44-67). As disclosed by Smithies et al., the transcript
21 generator module will perform session verification functions upon the transcript, such as
22 verification of signatures and verification of the transcript checksum. Further, as

disclosed by Smithies et al., with reference to claim 19, the transcript generator module and other supporting system components are implemented as programs.

Regarding claim 21, the combination of DeSimone et al. and Smithies et al. discloses a program means for controlling transmission of a request to a plurality of users to each attach a digital signature to a recording of said selection of message entries from a messaging session. (Smithies et al., Col. 41, lines 21-36, Col. 44, lines 46-56). In the program means, as disclosed by Smithies et al., multiple parties, or users, can engage in the generation of a transcript. The transcript generator module will request participants to the session to provide their digital signatures to the transcript.

Regarding claim 23, the combination of DeSimone et al. and Smithies et al. discloses a program means for calculating a checksum for a recording of a selection of message entries from a messaging session; and means for enabling encryption of the checksum utilizing a private key for a particular digital signature from among a plurality of digital signatures, wherein a particular public key enabled to decrypt the encrypted checksum (Smithies et al., Col. 8, lines 24-43; Col. 14, lines 26-39).

Regarding claim 24, the combination of DeSimone et al. and Smithies et al. discloses a program means for verifying an integrity of a selection of a plurality of message entries by calculating a current checksum for the selection of the plurality of message entries; decrypting said encrypted checksum with a particular public key; and

1 comparing the current checksum with the decrypted checksum, wherein the integrity is
2 verified if the decrypted checksum matches the current checksum (Smithies et al., Col.
3 14, lines 26-39).

4
5 Regarding claim 25, the combination of DeSimone et al. and Smithies et al.
6 discloses a program means for verifying a particular digital signature from among a
7 plurality of digital signatures in order to verify a particular user from among a plurality of
8 users associated with the particular digital signature (Smithies et al., Col. 41, lines 7-13,
9 21-36).

10
11 Regarding claim 27, the combination of DeSimone et al. and Smithies et al.
12 discloses a method for attaching a digital signature for a sender of a message entry to
13 the message entry; and distributing the message entry to a plurality of participants in a
14 messaging session, wherein each of the plurality of participants in the messaging
15 session are enabled to verify the message entry with the digital signature in real-time
16 (Smithies et al., Col. 13, lines 14-51; Col. 12, lines 14-16, 51-54; Col. 14, line 65 – Col.
17 15, line 4; Col. 41, lines 24-36). As disclosed by Smithies et al., messages created by
18 an individual through a client application are 'affirmed' (i.e. digitally signed) by the
19 individual. They are then added to the transcript, where other participants through their
20 respective client applications can view the transcript of messages, verify signatures of
21 the messages, and add their own messages.

1 Regarding claim 28, the combination of DeSimone et al. and Smithies et al.
2 discloses a method for attaching a digital signature for a sender at a client messaging
3 system before distribution within a network (Smithies et al., Fig. 1, Col. 8, lines 15-40;
4 Col. 41, lines 21-36). As shown by Smithies et al., when the client application and the
5 transcript generator module both reside on the client system, then the digital signatures
6 will be attached at the client system.

7
8 Regarding claim 29, the combination of DeSimone et al. and Smithies et al.
9 discloses a method for attaching a digital signature for a sender at a messaging server
10 before distribution to a plurality of participants (Smithies et al., Fig. 2, Col. 3, lines 40-61;
11 Col. 9, lines 56-63; Col. 41, lines 21-36). As shown by Smithies et al., the transcript
12 generator module may reside on a system other than a client system that has access to
13 it. In this case, digital signatures from a plurality of interacting client systems will be
14 attached at the messaging server system.

15
16 Regarding claim 30, the combination of DeSimone et al. and Smithies et al.
17 discloses a method for verifying at least one of an identity of a sender and an integrity of
18 content of said message entry (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col. 11,
19 lines 44-67; Col. 13, lines 14-45; Col. 14, line 65 – Col. 15, line 4). As disclosed by
20 Smithies et al., a user via a client application can utilize the transcript generator module
21 to perform session verification functions upon the transcript, such as verification of
22 statements ('message entries') and their corresponding signatures.

1
2 Regarding claim 31, the combination of DeSimone et al. and Smithies et al.
3 discloses a messaging system means for attaching a digital signature for a sender of a
4 message entry to the message entry; and means for distributing the message entry to a
5 plurality of participants in a messaging session, wherein each of the plurality of
6 participants in the messaging session are enabled to verify the message entry with the
7 digital signature in real-time (Smithies et al., Col. 13, lines 14-51; Col. 12, lines 14-16,
8 51-54; Col. 14, line 65 – Col. 15, line 4; Col. 41, lines 24-36). As disclosed by Smithies
9 et al., messages created by an individual through a client application are 'affirmed' (i.e.
10 digitally signed) by the individual. They are then added to the transcript, where other
11 participants through their respective client applications can view the transcript of
12 messages, verify signatures of the messages, and add their own messages.

13
14 Regarding claim 32, the combination of DeSimone et al. and Smithies et al.
15 discloses a system means for attaching a digital signature for a sender at a client
16 messaging system before distribution within a network (Smithies et al., Fig. 1, Col. 8,
17 lines 15-40; Col. 41, lines 21-36). As shown by Smithies et al., when the client
18 application and the transcript generator module both reside on the client system, then
19 the digital signatures will be attached at the client system.

20
21 Regarding claim 33, the combination of DeSimone et al. and Smithies et al.
22 discloses a system means for attaching a digital signature for a sender at a messaging

1 server before distribution to a plurality of participants (Smithies et al., Fig. 2, Col. 3, lines
2 40-61; Col. 9, lines 56-63; Col. 41, lines 21-36). As shown by Smithies et al., the
3 transcript generator module may reside on a system other than a client system that has
4 access to it. In this case, digital signatures from a plurality of interacting client systems
5 will be attached at the messaging server system.

6
7 Regarding claim 34, the combination of DeSimone et al. and Smithies et al.
8 discloses a system means for verifying at least one of an identity of a sender and an
9 integrity of content of said message entry (Smithies et al., Col. 9, line 64 – Col. 10, line
10 9; Col. 11, lines 44-67; Col. 13, lines 14-45; Col. 14, line 65 – Col. 15, line 4). As
11 disclosed by Smithies et al., a user via a client application can utilize the transcript
12 generator module to perform session verification functions upon the transcript, such as
13 verification of statements ('message entries') and their corresponding signatures.

14
15 Regarding claim 35, the combination of DeSimone et al. and Smithies et al.
16 discloses a program means for enabling attachment of a digital signature for a sender of
17 a message entry to the message entry; and means for controlling distribution of the
18 message entry to a plurality of participants in a messaging session, wherein each of the
19 plurality of participants in the messaging session are enabled to verify the message
20 entry with the digital signature in real-time (Smithies et al., Col. 13, lines 14-51; Col. 12,
21 lines 14-16, 51-54; Col. 14, line 65 – Col. 15, line 4; Col. 41, lines 24-36). As disclosed
22 by Smithies et al., messages created by an individual through a client application are

1 'affirmed' (i.e. digitally signed) by the individual. They are then added to the transcript,
2 where other participants through their respective client applications can view the
3 transcript of messages, verify signatures of the messages, and add their own
4 messages.

5
6 Regarding claim 36, the combination of DeSimone et al. and Smithies et al.
7 discloses a program means for enabling attachment of a digital signature for a sender at
8 a client messaging system before distribution within a network (Smithies et al., Fig. 1,
9 Col. 8, lines 15-40; Col. 41, lines 21-36). As shown by Smithies et al., when the client
10 application and the transcript generator module both reside on the client system, then
11 the digital signatures will be attached at the client system.

12
13 Regarding claim 37, the combination of DeSimone et al. and Smithies et al.
14 discloses a program means for enabling attachment of a digital signature for a sender at
15 a messaging server before distribution to a plurality of participants (Smithies et al., Fig.
16 2, Col. 3, lines 40-61; Col. 9, lines 56-63; Col. 41, lines 21-36). As shown by Smithies
17 et al., the transcript generator module may reside on a system other than a client
18 system that has access to it. In this case, digital signatures from a plurality of
19 interacting client systems will be attached at the messaging server system.

20
21 Regarding claim 38, the combination of DeSimone et al. and Smithies et al.
22 discloses a program means for verifying at least one of an identity of a sender and an

Art Unit: 2137

1 integrity of content of said message entry (Smithies et al., Col. 9, line 64 – Col. 10, line
2 9; Col. 11, lines 44-67; Col. 13, lines 14-45; Col. 14, line 65 – Col. 15, line 4). As
3 disclosed by Smithies et al., a user via a client application can utilize the transcript
4 generator module to perform session verification functions upon the transcript, such as
5 verification of statements ('message entries') and their corresponding signatures.

6
7
8 Claims 6, 10, 14, 18, 22, and 26 are rejected under 35 U.S.C. 103(a) as being
9 unpatentable over DeSimone et al. in view of Smithies et al., as applied to claims 1, 9,
10 11, 17, 19, and 25 above, and further in view of Schneier, Applied Cryptography.

11
12 Regarding claim 6, the combination of DeSimone et al. and Smithies et al.
13 discloses a method, system, and program for recording a verifiable messaging session.
14 The messaging session comprises a plurality of users participating in the session. The
15 participating users are able to view the history of the messaging session in the form of a
16 'conversation', a string of recorded messages (DeSimone et al., Col. 2, lines 48-56; Col.
17 3, lines 43-53). They disclose the recording of a verifiable transcript of statements,
18 transactions, or events between parties by attaching digital signatures of the
19 participants to the transcript (Smithies et al., Col. 3, lines 40-61; Col. 41, lines 21-36).
20 Further more, they disclose a signature verification system for the verification of digital
21 signatures that are associated with a plurality of users who participate in the generation
22 of a messaging session (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col. 11, lines

1 44-67). The combination of DeSimone et al. and Smithies et al., however, does not
2 disclose the storing of the plurality of keys used by the signature verification system for
3 verifying the plurality of digital signatures belonging to the plurality of users.

4 Schneier discloses an authentication system using public-key cryptography
5 wherein a plurality of keys are stored for the verification of a plurality of digital
6 signatures belonging to a plurality of users (Pages 53 - 54). As disclosed by Schneier,
7 with public key cryptography, a host safely stores a plurality of keys that are used for
8 authentication ('verification') functions. Such keys must be safely stored so that they
9 may be used later for verification purposes.

10 It is obvious that any system utilizing public key cryptography to verify the digital
11 signatures of a plurality of users requires a system to manage the usage and storage of
12 such keys. Therefore, it would have been obvious to one ordinarily skilled in the art to
13 combine the method/system/program combination of DeSimone et al. and Smithies et
14 al. with the authentication/verification system of Schneier, because a
15 method/system/program that uses a plurality of public keys for verification requires a
16 system that manages and stores said keys.

17
18 Regarding claim 10, in view of the reasons given regarding claim 6, the
19 combination of DeSimone et al., Smithies et al., and Schneier discloses a method for
20 determining whether a public key received order to verify a particular digital signature
21 matches a public key coupled the particular digital signature; and in response to
22 determining a match, verifying a particular user associated with the particular digital

signature (Schneier, Page 54, steps 1 – 4). In step 3 of the authentication system, Schneier discloses the looking up of a particular public key coupled to a particular user, and then using that key to decrypt a message. Thus, a determination has been made to use the matching public key that is coupled to a user. In step 4, after performing a successful decryption, the identity of the user is verified.

Regarding claim 14, in view of the reasons given regarding claim 6, the combination of DeSimone et al., Smithies et al., and Schneier discloses a log file repository for storing a plurality of public keys each associated with one from among a plurality of digital signatures such that the plurality of public keys are accessible to a plurality of users for verifying a messaging session (Schneier, Page 53).

Regarding claim 18, in view of the reasons given regarding claim 6, the combination of DeSimone et al., Smithies et al., and Schneier discloses a system means for determining whether a public key received order to verify a particular digital signature matches a public key coupled the particular digital signature; and means for verifying a particular user associated with the particular digital signature, in response to determining a match (Schneier, Page 54, steps 1 – 4). In step 3 of the authentication system, Schneier discloses the looking up of a particular public key coupled to a particular user, and then using that key to decrypt a message. Thus, a determination has been made to use the matching public key that is coupled to a user. In step 4, after performing a successful decryption, the identity of the user is verified.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

Regarding claim 22, in view of the reasons given regarding claim 6, the combination of DeSimone et al., Smithies et al., and Schneier discloses a program means for enabling storage of a plurality of keys each associated with one from among a plurality of digital signatures such that the plurality of public keys are accessible to a plurality of users for verifying a messaging session (Schneier, Page 53).

Regarding claim 26, in view of the reasons given regarding claim 6, the combination of DeSimone et al., Smithies et al., and Schneier discloses a program means for determining whether a public key received order to verify a particular digital signature matches a public key coupled the particular digital signature; and means for verifying a particular user associated with the particular digital signature, in response to determining a match (Schneier, Page 54, steps 1 – 4). In step 3 of the authentication system, Schneier discloses the looking up of a particular public key coupled to a particular user, and then using that key to decrypt a message. Thus, a determination has been made to use the matching public key that is coupled to a user. In step 4, after performing a successful decryption, the identity of the user is verified.

Response to Arguments

Applicant's arguments filed 4/25/2005 have been fully considered but they are not persuasive. Applicant argues primarily that:

i. "Claims 1-5, 7-9, 11-13, 15-17, 19-21, 23-25, and 27-38 are not obvious under the combination of DeSimone and Smithies" for the following reasons:

a. "There is no suggestion or motivation to modify DeSimone by Smithies", and "absent such a showing, the Examiner has impermissibly used hindsight occasioned by Applicants' own teaching to reject the claims" (Applicant's Remarks, pages 17, 18).

b. "First, there is not a suggestion or motivation to modify DeSimone in view of Smithies because when DeSimone is viewed as a whole, DeSimone only suggests that policies control which users can be added as new participants to a conversation, and not that "messaging session between users may need measures of security provided" " (Applicant's Remarks, page 19).

c. "Second, there is not a suggestion or motivation to modify DeSimone in view of Smithies because even if DeSimone teaches "the understanding that certain messaging sessions between users may need measures of security provided" as asserted by the Examiner, DeSimone only teaches applying security to limit those users who can add to a conversation, which does not suggest or motivate modifying DeSimone to teach attaching

1 digital signatures to a recording of a messaging session so that the participants
2 in the messaging session are verifiable.” (Applicant’s Remarks, page 20).

3 d. “There is no reasonable expectation of success in the proposed
4 modification of DeSimone by Smithies” (Applicant’s Remarks, page 21).

5 e. “Because prima facie obviousness is not established for claims 1,
6 11, and 19, at least by virtue of their dependency on claims 1, 11, and 19,
7 dependent claims 2-5, 7-9, 12-13, 15-17, 20-21, and 23-25 are not obvious in
8 view of DeSimone and Smithies, alone or in combination, under 35 U.S.C.
9 103(a)” (Applicant’s Remarks, page 21).

10 f. “Applicants note that the Examiner cites the combination of
11 DeSimone and Smithies as disclosing the elements of claim 27, but the Examiner
12 does not point to any specific teaching in DeSimone as grounds for the rejection.
13 Applicants traverse the grounds of rejection in view of the references to Smithies
14 cited by the Examiner. In addition, as to the combination of DeSimone and
15 Smithies, Applicants respectfully assert the arguments made with reference to
16 claim 1, as to the lack of motivation or suggestion for the combination of
17 DeSimone and Smithies and the lack of reasonable expectation of success in the
18 proposed modification, also apply to claims 27, 31, and 35, as a result prima
19 facie obviousness is not proved for claims 27, 31, and 35 and Applicants
20 respectfully request allowance of these claims” (Applicant’s Remarks, pages 21,
21 22).

1 g. “Neither DeSimone nor Smithies, separately or in combination,
2 teaches or suggests all the limitations of claims 27, 31, and 35” because
3 “Smithies does not teach that “messages created by an individual through a
4 client application are ‘affirmed’ (i.e. digitally signed) by the individual. They are
5 then added to the transcript, where other participants through their respective
6 client applications can view the transcript of messages, verify signatures of the
7 messages, and add their own messages.” [Office Action, pp. 11-12]” (Applicant’s
8 Remarks, pages 23).

9 h. “In addition, because prima facie obviousness is not established for
10 claims 27, 31, and 35, at least by virtue of their dependency on claims 27, 31,
11 and 35, dependent claims 28-30, 32-34 and 36-38 are not obvious in view of
12 DeSimone and Smithies, alone or in combination, under 35 U.S.C. §103(a).
13 Because a prima facie case of obviousness is not established for claims 28-30,
14 32-34, and 36-38, Applicants respectfully request allowance of claims 28-30, 32-
15 34, and 36-38” (Applicant’s Remarks, page 25).

16
17 ii. Claims 6, 10, 14, 18, 22, and 26 are not obvious under the combination of
18 DeSimone, Smithies, and Scheider” (Applicant’s Remarks, page 25) for the
19 following reason:

20 a. “Claims 6, 10, 14, 18, 22, and 26 stand rejected under 35 U.S.C.
21 §103(a) as being unpatentable over DeSimone in view of Smithies as
22 applied to claims 1, 9, 11, 17, 19, and 25 above, and further in view of

Art Unit: 2137

1 Schneider, Applied Cryptography. [Office Action. p. 16] Application
2 respectfully assert that because prima facie obviousness is not
3 established for claims 1, 11, and 19 under the combination of DeSimone
4 and Smithies, at least by virtue of their dependency on claims 1, 11, and
5 19, claims 6, 10, 14, 18, 22, and 26 are not obvious under the combination
6 of DeSimone and Smithies and Applied Cryptography under 35 U.S.C.
7 §103(a). Because a prima facie case of obviousness is not established for
8 claims 6, 10, 14, 18, 22, and 26, Applicants respectfully request allowance
9 of claims 6, 10, 14, 18, 22, and 26.

10
11
12 In response to applicant's argument i(a) that there is no suggestion to combine
13 the references, the examiner recognizes that obviousness can only be established by
14 combining or modifying the teachings of the prior art to produce the claimed invention
15 where there is some teaching, suggestion, or motivation to do so found either in the
16 references themselves or in the knowledge generally available to one of ordinary skill in
17 the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re*
18 *Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, DeSimone et al.
19 presents a system for participating and transcribing a messaging session. Particularly,
20 DeSimone et al. describes a chat messaging session and a transcript of the messaging
21 session (DeSimone et al., col. 2, lines 53-56). Smithies et al. describes a digitally
22 signed transcript of communications between parties. Smithies et al. teaches that it is

1 advantageous for purposes of security to digitally sign the transcript with the signatures
2 of the parties, providing a level assurance of the integrity of the transcript (Smithies et
3 al., Abstract; col. 3, lines 40-61; col. 8, lines 2-5; col. 13, lines 33-45; col. 14, lines 48-
4 67; col. 15, line 66 – col. 16, line 16; cols. 19,20,21,22). Thus, it would have been
5 obvious to one of ordinary skill in the art to employ the method of Smithies et al. for a
6 digitally signed transcript with the system of a messaging session and transcript by
7 DeSimone et al. This would have been obvious because one of ordinary skill in the art
8 would have been motivated to provide a level of assurance of the integrity of a transcript
9 for the purposes of security.

10 The examiner points out that a supplemental motive to the above mentioned
11 combination for providing security to a message transcript via verification may also be
12 found in DeSimone et al. itself. As stated, “DeSimone et al., *however*, does teach the
13 understanding that certain messaging sessions between users may need measures of
14 security provided” (italics added, Office Action, page 3). DeSimone et al. recognizes
15 that messaging sessions differ in the nature of the conversations. For example, some
16 messaging sessions recorded in a transcript are of a purely social and considerably
17 relaxed context. Others are not, and they require measures of security to be taken.
18 DeSimone et al.’s teaching regarding the differing nature of messaging sessions that
19 are recorded in a transcript gives evidence that they must at times be handled in ways
20 to provide for the security of the messaging session and, thus, the resulting transcript.
21 Therefore, this motive to provide security to a messaging session and resulting
22 transcript is supplemental to the motivation clearly shown in both the reference of

1 Smithies et al. and in the knowledge generally available to one of ordinary skill in the
2 art.

3 The applicant, however, has argued against the reference of DeSimone
4 individually by asserting that the teaching of DeSimone et al. for requirements of
5 security with respect to messaging sessions can only be applied in the context of
6 policies governing the allowance of participants into a messaging session. Therefore,
7 the examiner would like to reiterate that DeSimone has demonstrated that messaging
8 sessions recorded in a transcript differ in nature, from being relaxed and social to ones
9 requiring security measures. In response to applicant's arguments against the
10 references individually, one cannot show nonobviousness by attacking references
11 individually where the rejections are based on combinations of references. See *In re*
12 *Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091,
13 231 USPQ 375 (Fed. Cir. 1986).

14 Thus, the applicant's argument i(a) that there is no suggestion to combine the
15 references of DeSimone et al. and Smithies et al. is unpersuasive.

16 Further, in response to applicant's argument i(a) that the examiner's conclusion
17 of obviousness is based upon improper hindsight reasoning, it must be recognized that
18 any judgment on obviousness is in a sense necessarily a reconstruction based upon
19 hindsight reasoning. But so long as it takes into account only knowledge which was
20 within the level of ordinary skill at the time the claimed invention was made, and does
21 not include knowledge gleaned only from the applicant's disclosure, such a

1 reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA
2 1971).

3
4 In response to applicant's arguments i(b) and i(c), they are shown to be
5 unpersuasive for the reasons supplied in the response to applicant's argument i(a).

6
7 In response to applicant's argument i(d), that there is no reasonable expectation
8 of success in the proposed modification of DeSimone et al. by Smithies et al., examiner
9 notes that the applicant has based this argument on the preceding arguments of a lack
10 of motivation to combine. Thus, this argument is shown to be unpersuasive for the
11 reasons supplied in the response to applicant's arguments i(a).

12
13 Applicant's argument i(e) is based upon the unpersuasive arguments preceding
14 it, and therefore, argument i(e) is shown to be unpersuasive for the reasons supplied in
15 the response to applicant's arguments i(a).

16
17 In response to applicant's argument i(f), the examiner points out that the rejection
18 was made upon the grounds of the combination of DeSimone et al. and Smithies et al.,
19 as previously stated in the examiner's first office action. Further, the applicant's
20 argument i(f) is based upon the unpersuasive arguments i(a-d), and therefore, argument
21 i(f) is also shown to be unpersuasive for the reasons supplied in the response to
22 applicant's arguments i(a-d).

1
2 Regarding the applicant's argument i(g), that neither DeSimone nor Smithies,
3 separately or in combination, teaches or suggests all the limitations of claims 27, 31,
4 and 35, the applicant provides the following reason: "Smithies does not teach, however,
5 the assertions made by the Examiner as to its teaching and its teaching do not teach
6 the elements of claim 27. The Examiner incorrectly asserts that the affirmed document
7 or "message" is added to the transcript, where other participants can view the transcript
8 of messages, verify signatures of the messages, and add their own messages. In
9 particular, Smithies teaches that documents are affirmed by an individual and that the
10 responses during the affirmation process are stored in a transcript object; the document
11 or "message" is not stored in the transcript" (Applicant's Remarks, page 24).

12 In response to this argument, the examiner points out that the applicant has
13 misinterpreted the examiner's rejection. First, the examiner has not asserted that the
14 affirmed document is the equivalent to the "message". Second, the examiner has not
15 asserted that the affirmed document is stored in the transcript object. Smithies et al.
16 demonstrates a system for allowing a plurality of parties to engage in a messaging
17 session of interactions, such as statements and affirmations, concerning a particular
18 subject such as a transaction, event, or document. The session is recorded in a
19 transcript and associated with digital signatures for the security of the messaging
20 session, allowing the participants to be verified (Smithies et al., Abstract; col. 3, lines
21 40-61; col. 8, lines 2-5; col. 13, lines 33-45; col. 14, lines 48-67; col. 15, line 66 – col.
22 16, line 16; cols. 19,20,21,22).

1 In addition, regarding this argument, the examiner points out that the applicant
2 has mischaracterized the reference of Smithies et al. Namely, the applicant asserts:
3 “Where multiple individuals affirm a document, a separate transcript object is created for
4 each affirmation; individuals do not open an affirmation transcript (transcript object) and
5 add their own documents or “messages” to that transcript object” (Applicant’s Remarks,
6 page 24). On the contrary, Smithies discloses that a transcript object is passed
7 between the application clients of the plurality of parties. During the messaging
8 (“affirmation”) session, the parties may verify the signatures associated with the
9 transcript that is stored in the transcript object, but they may not change anything
10 previously recorded in the transcript. Thus, while the parties are enabled to make
11 identical copies of the transcript object and the transcript contain therein, the parties
12 may not change the transcript and thereby create a separate or unrelated transcript
13 object. Smithies et al., further discloses that the parties may, in succession, add to the
14 record of the transcript object their own statements or affirmations (Smithies et al., fig. 2;
15 cols. 40, 41).

16 Finally, regarding this argument, the examiner points out that the rejection of
17 claim 27 was upon the grounds of the combination of DeSimone et al. and Smithies et
18 al. As was shown by the examiner, the combination is specifically the method of
19 recording digital signatures of participants along with a messaging transcript (the
20 participants’ signatures being verifiable by viewers of the transcript) as taught by
21 Smithies et al. with the method of DeSimone et al. for enabling a messaging (“chat”)

1 session between users and the recording of a transcript (the transcript being viewable in
2 real time by the participants) of the session (Office Action, pages 2, 3).

3 Thus, the applicant's argument i(g) is shown to be unpersuasive, as the
4 combination of DeSimone et al. and Smithies et al. teaches the limitations of claims 27,
5 31, and 35.

6
7 In response to applicant's arguments i(h), it is shown to be unpersuasive for the
8 reasons supplied in the response to applicant's argument i(g).

9
10 In response to applicant's arguments i(h), it is shown to be unpersuasive for the
11 reasons supplied in the response to applicant's argument i(g).

12
13 In response to applicant's arguments ii(a), the argument is based solely upon the
14 preceding unpersuasive arguments and it is shown to be unpersuasive for the reasons
15 supplied in the responses above to applicant's arguments i(a-g).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Art Unit: 2137

1 Information regarding the status of an application may be obtained from the
2 Patent Application Information Retrieval (PAIR) system. Status information for
3 published applications may be obtained from either Private PAIR or Public PAIR.
4 Status information for unpublished applications is available through Private PAIR only.
5 For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should
6 you have questions on access to the Private PAIR system, contact the Electronic
7 Business Center (EBC) at 866-217-9197 (toll-free).

8
9
10 Jeffery Williams
11 Assistant Examiner
12 Art Unit 2137
13 7.13.2005

Matthew L. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137